REMARKS/ARGUMENTS

Claims 1-67 are currently pending in this application. Claims 1, 22, 44, and 56 have been amended. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reconsideration and an early indication of allowance of claims 1-67 are respectfully requested.

The specification has been amended to correct certain informalities. The amendments do not add any new matter. Entry of the amendments is respectfully requested.

Claims 1-3, 5-12, 15, 17-24, 26-33, 35-40, 43-46, 48-49, 51-52, 55-58, 60-61, and 63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (U.S. Patent No. 6,769,063) in view of Callum (U.S. Patent No. 6,320,964) and Kamishima (U.S. Patent No. 6,236,686). Claims 4, 13-14, 25, 41-42, 47, 53-54, 59 and 65-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and further in view of Steinman et al. (U.S. Patent No. 6,591,349). Claims 16, 34, 50, and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and Steinman, and in further view of Teppler (U.S. Patent No. 6,792,536). Applicant respectfully traverses these rejections.

Claims 1 and 44 have been amended to recite a "permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block, wherein the second bit sequence is derived from R XOR $P^{-1}(L)$, where R is a third bit sequence

-18-

based on the expanded first bit sequence, and $P^{-1}(L)$ is an inverse permutation of a bit sequence corresponding to a second portion of the data block, the inverse permutation being performed by an inverse permutation logic performing reverse operations of the permutation logic." Support for this amendment may be found on FIGS. 5 and 6 of the drawings, and on page 16, line 29 through page 19, line 18 of the specification, especially on page 18, lines 3-7.

None of the cited references teach or suggest the claimed permutation logic. Although Kanda discloses a permutation part 19 on FIG. 2, the permutation part is included in a timing critical data path that includes an expanded permutation part 17 expanding a 32-bit block data to a 48-bit data, XOR circuit 18 combining the 48-bit data with a key, and S-boxes S0-S7 transforming the data output of the XOR circuit to a 32-bit data and providing the 32-bit data to the permutation part 19. (See, Col. 2, lines 22-39). In contrast, the invention claimed in claims 1 and 44 allows the permutation logic to reside outside the timing critical data path and increases throughput. Accordingly, claims 1 and 44 are now in condition for allowance.

Claims 22 and 56 have been amended back to their original wording. Claims 22 and 56 recite an "inverse permutation logic coupled to the input stage of the multiplexer circuitry, the inverse permutation logic performing reverse operations of the permutation logic." The Examiner relies on FIG. 3, reference number 311 of Callum to contend that it teaches the recited "inverse permutation logic." Applicant respectfully disagrees.

The item referenced with reference number 311 in Callum is

associated with an initial permutation operation. (See, Col. 4, lines 14-18). There is no indication in Callum or in any of the other cited references that this initial permutation operation performs "reverse operations of the permutation logic" as is required by claims 22 and 56. Accordingly, claims 22 and 56 are in condition for allowance.
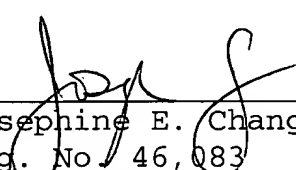
Claims 2-21, 23-43, 45-55, and 57-67 are also in condition for allowance because they depend on an allowable base claim, and for the additional limitations contained therein.

In view of the above amendments and remarks, Applicant respectfully requests an early indication of allowance of claims 1-67.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Josephine E. Chang
Reg. No. 46,083
626/795-9900

JEC/lal
LAL PAS621072.1-*-05/2/05 4:46 PM